29.01.99.E1.27 Exclusions from Required Risk Mitigation Measures

Approved September 25, 2009
Revised June 5, 2013
Next Schedule Review: June 5, 2016

Supplements TEES Rule 29.01.99.E1

Standard Administrative Procedure Statement
The scope of this procedure is to handle exceptions that resource owners determine are not essential for an information resource and/or environment.

Reason for Standard Administrative Procedure
The purpose of this procedure is to provide an exception process for information resource risk mitigation requirements.

Procedures and Responsibilities

1. CONTROLS AND RESPONSIBILITIES

   1.1 Exclusions are of two types:

      1.1.1 An exclusion may be granted to address the specific circumstances or business needs relating to an individual program or division. Requests for exclusions of this type are to be initiated by the information resource owner or their designee.

      1.1.2 Broader exclusions may be issued to address circumstances that span the Agency as a whole. Requests for exclusions of this type may come from any person, or may be initiated by the Chief Information Officer (CIO). Exclusions of this type will be documented in each SAP to which the exclusion applies.

   1.2 Exclusions requested by the information resource owner must be submitted through an exclusion request. The request must contain the following:

      1.2.1 Provision for which the exclusion is sought.

      1.2.2 A statement defining the nature and scope of the exclusion in terms of the data included and/or the class of devices included.

      1.2.3 Risk management rationale for the exclusion.
1.3 Each request will be reviewed by the CIO or designee. After any questions or concerns are addressed, the requestor will be notified as to whether the request was approved or denied. A record of all requests and results will be maintained by the CIO or designee.

1.4 If the request is denied, a rationale for the denial will be supplied to the requestor.

1.5 If the request is approved:

1.5.1 The information resource owner may be required to apply compensating security controls to mitigate any risk resulting from the exclusion.

1.5.2 An expiration date for the exclusion will be supplied to the requestor.

1.5.3 The request for the exclusion will be fully documented in ISAAC in the form of a risk management decision by the information resource owner or their designee.

Related Statutes, Policies, or Requirements
TAMU SAP 29.01.99.M1.27, Information Resources - Exclusions from Required Risk Mitigation Measures

Texas Administrative Code 202

TEES Rule 29.01.99.E1, Security of Electronic Information Resources

Contact Office
Information Technology Services
(979) 847-8585